

1 PACHULSKI STANG ZIEHL & JONES LLP
2 Debra I. Grassgreen (CA Bar No. 169978)
3 Jason H. Rosell (CA Bar No. 269126)
4 One Sansome Street, Suite 3430
5 San Francisco, California 94104
Telephone: (415) 263-7000
Facsimile: (415) 263-7010
E-mail: dgrassgreen@pszjlaw.com
jrosell@pszjlaw.com

6 *Counsel to the Debtor*

7 **UNITED STATES BANKRUPTCY COURT**
8 **NORTHERN DISTRICT OF CALIFORNIA**
9 **SAN FRANCISCO DIVISION**

10 In re:

11 INTERNATIONAL LONGSHORE
12 AND WAREHOUSE UNION,

13 Debtor.

14 Case No. 23-30662-HLB

15 Chapter 11

16 **DECLARATION IN SUPPORT OF
17 EMPLOYMENT OF FTI CONSULTING
18 (SC) INC. AS PROFESSIONAL UTILIZED
19 IN THE ORDINARY COURSE OF
20 BUSINESS**

21 I, Jennifer E. Mercer, pursuant to 28 U.S.C. § 1746, declare that the following is true to the
22 best of my knowledge, information, and belief:

23 1. I am a Managing Director of FTI Consulting (SC) Inc., located at 555 12th Street NW,
24 Suite 700, Washington DC 20004 (the “Firm”), which has been employed by the debtor and debtor in
possession (the “Debtor”) in the above-captioned case (the “Chapter 11 Case”) in the ordinary course
of the Debtor’s business. The Debtor wishes to retain the Firm to continue providing ordinary course
services during the Chapter 11 Case, and the Firm has consented to provide such services. This
declaration is submitted in compliance with the *Order Approving Debtor’s Motion for Entry of Order*
(*I*) *Authorizing Employment and Payment of Professionals Utilized in the Ordinary Course of Business*
and (*II*) *Granting Related Relief* (the “Ordinary Course Professionals Order”).

25 2. The Firm may have performed services in the past, may currently perform services, and
26 may perform services in the future in matters unrelated to the Chapter 11 Case for persons that are
27 parties in interest in the Chapter 11 Case. The Firm does not perform services for any such person in

connection with the Chapter 11 Case or have any relationship with any such person, their attorneys, or their accountants that would be adverse to the Debtor or its estate.

3. The Debtor has requested that the Firm provide strategic and crisis communications services to the Debtor, and the Firm has consented to provide such services.

4. The Firm has provided services to the Debtor prior to the commencement of the Chapter 11 Case.

5. As part of its customary practice, the Firm is retained in cases, proceedings, and transactions involving many different parties, some of whom may represent or be employed by the Debtor, claimants, and parties in interest in the Chapter 11 Case.

6. Neither I nor any principal, partner, director, or officer of, or professional employed by, the Firm has agreed to share or will share any portion of the compensation to be received from the Debtor with any other person other than the principal and regular employees of the Firm.

7. Neither I nor any principal, partner, director, or officer of, or professional employed by, the Firm, insofar as I have been able to ascertain, holds or represents any interest adverse to the Debtor or its estate with respect to the matter(s) upon which the Firm is to be employed.

8. The Debtor owes the Firm \$0.00 for fees and expenses incurred prior to the date the Chapter 11 Case was commenced (the “Petition Date”), the payment of which is subject to the limitations contained in the Bankruptcy Code and any orders of the Court.

9. As of the Petition Date, the Firm held a prepetition retainer of \$ 75,000.00.

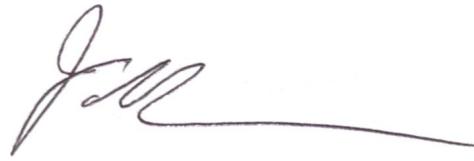
10. As of the Petition Date, the Firm was party to an agreement for indemnification with the Debtor. A copy of such agreement is attached as **Exhibit A** to this Declaration.

[*Remainder of Page Intentionally Left Blank*]

1 11. The Firm is conducting further inquiries regarding its retention by any creditors of the
2 Debtor, and upon conclusion of such inquiries, or at any time during the period of its employment, if
3 the Firm should discover any facts bearing on the matters described herein, the Firm will supplement
4 the information contained in this Declaration.

5 I declare under penalty of perjury under the laws of the United States of America that the
6 foregoing is true and correct.

7
8 Dated: 12/7/2023



9 Jennifer E. Mercer
10 Managing Director
11 FTI CONSULTING (SC) INC.
12 Address: 555 12th Street NW, Suite 700,
13 Washington DC 20004
14 Telephone: (202) 402-1588
15 Email: jennifer.mercer@fticonsulting.com

Exhibit A



Strategic Communications
 555 12th Street NW, #700, Washington, DC 20004
 T +1 (202) 312-9100 F +1 (202) 312-9101

September 12, 2023

Lindsay R. Nicholas
 ILWU General Counsel & Executive Administrator
 1188 Franklin Street, 4th Floor
 San Francisco, CA 94109

This letter shall serve to confirm our Agreement as follows:

1. International Longshore and Warehouse Union ("ILWU" or "Client") hereby retains FTI Consulting (SC) Inc. ("FTI") effective as of September 12, 2023 to provide multi-stakeholder restructuring communications and contingency planning support, as well as any other strategic communications support required for ILWU. The Services may be performed by FTI or by any subsidiary or affiliate of FTI, as FTI shall determine. References herein to FTI and its employees shall be deemed to apply also, unless the context shall otherwise indicate, to employees of each such subsidiary, affiliates parties and their employees.
2. The initial term of this Agreement shall be for the period commencing on September 12, 2023 and shall continue through the restructuring ("Initial Term") unless otherwise terminated by either party upon fifteen days prior written notice to the other party.
3. As compensation for the services to be rendered by FTI hereunder during the Initial Term of the Agreement, FTI will collect an initial fee of \$75,000 with staff hours billed against this fee on an hourly basis at the rates below. On a regular basis, FTI will calculate the time input by staff and deduct that amount from the initial fee. If the initial fee is exhausted, FTI will update Client and propose an additional go-forward fee replenishment to ensure disinterestedness as the case progresses (in concert with Ordinary Course Professional procedures and caps, as applicable in a post-petition context).

FTI Hourly Charge-Out Rates

Sr. Managing Director/Sr. Advisor	\$950/hour
Managing Director	\$800/hour
Sr. Director	\$700/hour
Director	\$600/hour
Sr. Consultant	\$475/hour
Consultant	\$375/hour
Administration	\$150/hour

FTI's rates are subject to adjustment from time to time and at least annually effective January 1. FTI will advise Client immediately if a rate adjustment is being made.

4. Client shall be responsible for all reasonable and necessary disbursements made by FTI on behalf of Client, including travel and meals expenses. In addition, specific periodic expenses include:

A one-time charge of \$400.00, which represents FTI's costs associated with the multiple data sources that are required to facilitate daily program activities such as news retrieval access, analyst reports, and financial and industry publications, as well as FTI's costs associated with account administration.

In addition, FTI shall also charge the Client an additional highly specialized research ("HSR") fee under any of the following three (3) scenarios outlined below. FTI will provide the Client with advance notice of any applicable fee(s) before beginning the workstream or project in question.

- (HSR-1) – In the case where work being performed requires FTI to conduct a quantitative media or social media landscape analysis, a one-time fee of \$3,000 will be charged to the Client.



- (HSR-2) – In the case where work being conducted related to any type of quantitative media analysis requires FTI to employ its proprietary data science techniques, technology, and/or platforms, a one-time fee of \$7,500 will be charged to the Client.
- (HSR-3) – In the case where work being conducted is related in part or full to an Environmental, Social, and Governmental (ESG) assessment, materiality assessment, peer benchmarking or related research, a one-time fee of \$2,500 will be charged to the Client.

FTI shall bill Client, and Client shall reimburse FTI for all expenses and disbursements made on behalf of Client. FTI will charge these expenses against the initial fee of \$75,000. All expenses and disbursements incurred after exhaustion of the initial fee will be itemized in each monthly invoice.

In situations where a third-party supplier requires prepayment of part or all of its fees before providing materials and services (such as media), Client agrees to either pay such third party supplier directly when due or pay FTI the amounts required by the third party supplier in order for FTI to pay such amounts to the third party supplier when due. FTI will not be obligated to proceed with such projects if such payments have not been made, or if FTI is required to become liable to the third-party supplier before receipt of such payment from Client.

5. Invoices are due and payable upon receipt. The name and address of the Client designee to receive and approve FTI's invoices is indicated on the signature page of this letter. Client agrees to pay all court costs, attorney fees (whether or not contingent on collection from Client) and other expenses which may be associated with the collection of unpaid invoices. In addition to the remedies set forth above and any other remedies available at law, FTI reserves the right to defer rendering further services until payment is received on past-due invoices.
6. Client will furnish to FTI certain material, non-public information concerning Client. As a condition of receiving such information, FTI agrees to treat any such information concerning Client, which is furnished to FTI by or on behalf of Client (herein collectively referred to as the "Information") in accordance with the provisions of this agreement. The term "Information" does not include Information which (a) was or becomes generally available to the public other than as a result of a disclosure by FTI or its directors, officers, employees, agents or advisors, (b) was available prior to its disclosure to FTI by Client or its representatives, (c) becomes available on a non-confidential basis from a source other than Client or its representatives, provided that such source is not known by FTI to be subject to another confidentiality agreement with or another obligation of secrecy to Client or another party, or (d) is independently developed by FTI.

FTI hereby agrees that the Information will be kept confidential by FTI for a period of three years following the receipt of such Information (except that Information that qualifies as a trade secret shall be kept confidential for as long as such Information remains a trade secret under applicable law) and will not be disclosed to any outside party except as so directed by Client. This provision shall survive the expiration or termination of this Agreement.

If FTI is requested or required (by oral questions, interrogatories, requests for Information or documents, subpoena, Civil Investigative Demand or similar process) to disclose any Information supplied to FTI in the course of dealings with Client, it is agreed that, to the extent permitted by law, FTI will provide Client with prompt notice of such request or requirement so that Client may seek an appropriate protective order and/or waive compliance with the provisions of this Agreement. It is further agreed that if, in the absence of a protective order or the receipt of a waiver hereunder, FTI is nonetheless, in the opinion of our counsel, required to disclose Information concerning Client to any tribunal or else stand liable for contempt or suffer other censure, penalty or other liability, FTI may disclose such Information to such tribunal without liability hereunder. If FTI and/or any of its employees are required to testify or provide evidence at or in connection with any judicial or administrative proceeding relating to this engagement to which FTI is not a party, Client will compensate FTI at its regular hourly rates and reimburse FTI for reasonable expenses (including counsel



fees) with respect thereto. The provisions of this paragraph shall survive the expiration or termination of this Agreement.

Upon the earlier of (a) two (2) years from the date of the final invoice issued hereunder or (b) upon written notice to the Client, FTI will, at its option, destroy or return to the Client all original materials provided by the Client to FTI, and all materials created by FTI specifically for the Client under this Agreement; provided, however, that with respect to back-up media, such materials will be overwritten or destroyed, subject to FTI's normal schedule for overwriting and destruction, as the case may be.

If this engagement involves the processing of personal data (also referred to herein as personal information) (i) as governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the terms of the EU Data Protection Schedule attached hereto as Schedule A shall apply to this engagement and it shall form an integral part of this Agreement and (ii) as governed by the California Consumer Privacy Act, the terms of the California Data Protection Schedule attached hereto as Schedule B shall apply to this engagement and it shall form an integral part of this Agreement. In the event of a conflict between the terms of this Agreement and the terms of Schedule A or Schedule B, the terms of Schedule A or Schedule B shall prevail in relation to the processing of such personal data. If such personal data is processed in connection with this engagement, Client shall notify FTI in writing before any personal data is disclosed to FTI.

During the course of performing services, FTI may collect, generate or obtain via license, data such as, but not limited to, communications performance data, media reports, social media, media analytics, primary research data, publicly available data, opt-in subscriber data, and target audience lists. Where FTI has not been provided this data by the client under the definition of confidential "information" (as defined in Section 6), FTI retains ownership of any and all rights to this data and its derivatives. However, FTI may not use this data in affiliation with the client's name for any purpose outside the scope of this agreement without prior, expressed written prior consent from the client.

7. Client agrees to promptly notify FTI if it extends (or solicits the possible interest in receiving) an offer of employment to an employee of FTI involved in this engagement and agrees that it will pay FTI a cash fee, upon hiring, equal to 100% of the aggregate current annualized compensation (both cash and non-cash consideration), including any guaranteed or target bonus, to be paid to FTI's former principal or employee that the Client or any of its subsidiaries or affiliates hires at any time up to one year subsequent to the date of the final invoice rendered by FTI with respect to this engagement; provided, however, the provision of this Section 7 shall not apply to any former principal or employee of FTI that contacts Client pursuant to a general solicitation of employment not directed at such principal or employee or that contacts Client on their own accord without any solicitation by Client.
8. FTI Consulting (SC) Inc. is a wholly owned subsidiary of FTI Consulting, Inc., a global firm with numerous worldwide practices. Affiliated entities of FTI may be engaged by parties with interests that are adverse to and may not be consistent with the interests of Client. Absent your prior approval, the FTI Consulting (SC) Inc. employees providing services hereunder will not provide services to a party that is adverse to Client in this matter. If employees of other FTI Consulting, Inc. entities provide services to Client as part of this engagement team in this matter, those employees will be subject to these same restrictions.
9. This Agreement constitutes the entire understanding and Agreement between the parties with respect to the subject matter covered herein and all prior or contemporaneous understandings, negotiations and agreements are herein merged.
10. The Agreement may not be altered, extended, or modified nor any of its provisions waived, except by a document in writing signed by the party against whom such alteration, modification, extension or waiver is sought to be enforced.
11. A waiver by either party of any breach, act or omission of the other party is not to be deemed a waiver of any subsequent similar breach, act or omission.



12. The terms and provisions of this Agreement shall be binding upon and shall inure to the benefit of each of us and our respective successors and assigns.
13. This Agreement shall be governed by the laws of the State of California, without giving effect to the choice of law provisions thereof. As to any dispute arising out of Paragraph 3, 4 or 5 it shall be subject to binding arbitration before the American Arbitration Association, California, before a single arbitrator whose decision will be final and binding. For all other terms of this agreement each party hereby agrees to jurisdiction and venue in the State or Federal courts in California. To facilitate judicial resolution and save time and expense, FTI and the Client irrevocably and unconditionally agree to waive a trial by jury in any action, proceeding or counterclaim arising out of or relating to this Agreement or the services provided hereunder. Client hereby waives personal service of process in any action or proceeding arising hereunder and Client agrees that such process shall be deemed properly and adequately served if sent to our address set forth in this Agreement, by certified or registered mail, return receipt requested.
14. Client agrees that FTI shall not be liable under this Agreement to Client, or its respective successors, assigns or affiliates for damages in excess of the total amount of the fees paid to FTI under this Agreement. In no event shall FTI be liable for punitive or consequential damages of any kind. Client shall indemnify FTI, and hold FTI harmless against any and all claims by third parties for losses, damages or liabilities, including reasonable attorney's fees and expenses ("Losses"), arising in any manner out of or in connection with this Agreement, unless it is finally judicially determined that such Losses resulted from the gross negligence or willful misconduct of FTI. The terms of this paragraph shall survive the termination of this Agreement and shall apply to any controlling person, director, officer, employee or affiliate of FTI.
15. This Agreement may be executed in counterparts. Electronic/PDF copies are as effective as the original.
16. All notices, requests, demands, or other communications under this Agreement shall be in writing, notice shall be sufficiently given for all purposes as follows:

Personal delivery. When personally delivered to the recipient, notice is effective on delivery.

Electronic mail. When successfully emailed to Brian Kennedy at the address of Brian.Kennedy@fticonsulting.com, notice is effective on receipt.

Certified mail. When mailed certified mail, return receipt requested, notice is effective on receipt, if delivery is confirmed by return receipt.

Overnight delivery. When delivered by overnight delivery Federal Express/Airborne/United Parcel Service/DHL Worldwide Express, charges prepaid or charged to the sender's account, notice is effective on delivery, if delivery is confirmed by the delivery service.

Addresses for purpose of giving notice are as follows:

To FTI: Attn: Brian Kennedy or CEO/COO/CFO
FTI Consulting (SC) Inc.
555 12th Street, NW
Suite 700
Washington DC 20004

To Client: Lindsay R. Nicholas
ILWU General Counsel & Executive Administrator
1188 Franklin Street, 4th Floor
San Francisco, CA 94109



17. If a court or an arbitrator of competent jurisdiction holds any provision of this Agreement to be illegal, unenforceable, or invalid, in whole or in part for any reason, the validity and enforceability of the remaining provisions, or portions of them, will not be affected, unless an essential purpose of this Agreement would be defeated by the loss of the illegal, unenforceable, or invalid provision.
18. The Client agrees that it will comply with all anti-corruption, anti-money laundering, anti-bribery and other economic sanctions laws and regulations of the United States, United Kingdom, European Union and United Nations (collectively, the "ABC/AML/Sanction Laws") in connection with this Agreement. The Client further agrees that it shall not, and it shall procure its employees not to, pay or cause other person(s) to pay FTI using any funds that would result in a violation of any of the ABC/AML/Sanction Laws by either Client or FTI, or otherwise take any action that would result in a violation of any of the ABC/AML/Sanction Laws by either Client or FTI. The Client shall promptly notify FTI in the event of any violation or failure to comply with ABC/AML/Sanction Laws in connection with this Agreement, or allegations relating thereto, by the Client or its directors, officers, employees or agents.

If the foregoing correctly sets forth the terms and conditions of our Agreement, please have the enclosed copy of this letter signed by a duly authorized officer beneath the words "Agreed to and Accepted" and return same to us

Agreed to and Accepted:

FTI Consulting (SC) Inc.

By: 
8FC9DB2CE95848D...
Chris Tucker
SMD, FTI Strategic Communications

Date: 9/18/2023

International Longshore and Warehouse Union (ILWU)

By: 74F1D3673A794C4...
Lindsay R. Nicholas
General Counsel & Executive Admin.
ILWU

Lindsay R. Nicholas
Syracuse University

Lindsay R. M.

Lindsay R. Nic

General Counsel & Executive Admin. ILWU

9/18/2023

Date:

DocuSigned by:

Elie R. Fagin

By: Edwin R. Ferris
Edwin R. Ferris
International Secretary-Treasurer

Date: _____

Name and Address of Client contact designated to receive and approve invoices related to this Agreement:

Name: Lindsay R. Nicholas, ILWU General Counsel and Executive Administrator
Address: 1188 Franklin Street, 4th Floor
San Francisco, CA 94109
Phone: 415.775.0533
E-Mail: Lindsay.Nicholas@ilwu.org



Schedule A

FTI CONSULTING DATA PROTECTION SCHEDULE

This Data Protection Schedule ("Schedule") forms part of the contract for services to which it is an attachment (the "Contract") between the client party identified in the Contract (the "Client") and the relevant FTI Consulting group entity identified in the Contract ("FTI").

1. Definitions

- 1.1 In this Schedule, unless otherwise defined herein, all defined terms shall have the meaning set out in the Contract.
- 1.2 In this Schedule, the following terms shall have the meanings set out below:
 - 1.2.1 "**Data Protection Laws**" means all legislation protecting the personal data of natural persons that is applicable to the processing of Personal Data under this Schedule, including (without limitation) the GDPR and any national legislation which supplements the GDPR, and the data protection laws of any other country, state or territory which apply to such processing;
 - 1.2.2 "**EEA Standard Contractual Clauses**" means the Standard Contractual Clauses set out in the European Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as updated, amended, replaced or superseded from time to time by the European Commission;
 - 1.2.3 "**GDPR**" means the General Data Protection Regulation (EU) 2016/679;
 - 1.2.4 "**Restricted Transfer**" means a transfer of Personal Data from Client to FTI in circumstances where such transfer would be prohibited by Data Protection Laws in the absence of the EEA or UK Standard Contractual Clauses;
 - 1.2.5 "**Standard Contractual Clauses**" means either the EEA or the EEA Contractual Clauses as amended by the IDTA, as applicable to a Restricted Transfer;
 - 1.2.6 "**UK IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018;
 - 1.2.7 "**UK GDPR**" means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019; and
 - 1.2.8 "**Personal Data**", "**Process**", "**Controller**", "**Processor**", "**Data Subject**", "**Supervisory Authority**" and "**Personal Data Breach**" shall have the meanings given to them in the Data Protection Laws.

2. Controller Terms

- 2.1 FTI and the Client will each act as separate and individual Controllers in relation to any Personal Data (including, without limitation, Personal Data relating to any of the Client's workers, FTI's workers, any



litigation or arbitration opponent or customer or vendor or transaction partner) Processed by the Client or FTI to deliver the services set out under the Contract.

- 2.2 FTI and the Client will each comply with its own respective obligations under the Data Protection Laws in relation to their Processing of Personal Data under the Contract. In particular, the Client will ensure that any disclosures of Personal Data to FTI are lawful, and, in each case where necessary under the Data Protection Laws, the Client has notified and secured the consent of the relevant Data Subjects.
- 2.3 FTI may appoint Processors as required to deliver the services, who will process the Personal Data on FTI's behalf and at FTI's direction. Further, FTI may disclose Personal Data to other Controllers:
 - 2.3.1 where necessary to deliver the services (including, but without limitation, law firms, accountants, other third party experts and any member of FTI's group of companies); or
 - 2.3.2 pursuant to a legally binding written request, an order or request of a court of competent jurisdiction or any governmental or regulatory authority or where disclosure is required by applicable law or regulation ("**Legal Process**"). In relation to any Legal Process, FTI shall assess the lawfulness of the request before responding, and shall take any steps required by Data Protection Laws to protect Personal Data prior to its disclosure (including, without limitation, with respect to data minimization and data security);
- 2.4 In respect of any Restricted Transfer subject to the GDPR, the parties hereby enter into Module 1 of the EEA Standard Contractual Clauses (with Client as data exporter and FTI as data importer), which is hereby incorporated by reference into this Schedule and which shall come into effect upon the commencement of a Restricted Transfer. The parties make the following selections for the purposes of Module 1:
 - 2.4.1 Clause 7 – *Docking clause* shall apply;
 - 2.4.2 Clause 11(a) – *Redress* the optional language shall not apply;
 - 2.4.3 Clause 13(a) – *Supervision*
 - 2.4.3.1 Where Client is established in an EU Member State, the following shall apply: "The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall be the supervisory authority of the Member State in which Client is established or (if different) the lead supervisory authority of the Client in respect of a cross-border processing activity". OR
 - 2.4.3.2 Where Client is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR the following shall apply: "The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, shall act as competent supervisory authority." OR
 - 2.4.3.3 Where Client is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) without however having to appoint a representative the following shall apply: "The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or



whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority."

- 2.4.4 Clause 17 – *Governing law* “Option 1” shall apply and the “Member State” shall be the Republic of Ireland;
- 2.4.5 Clause 18 – *Choice of forum and jurisdiction* the Member State shall be the Republic of Ireland;
- 2.4.6 Annex 1 – the data exporter is Client and the data importer is FTI (in each case as identified, including in relation to their places of establishment, in the Principal Agreement) and the description of transfer is deemed to be as described in Annex 1 to this Schedule;
- 2.4.7 Annex 2 – the technical and organizational security measures are deemed to be as described in Annex 2 to this Schedule; and
- 2.4.8 Annex 3 – not applicable.

2.5 In respect of any Restricted Transfer subject to the UK GDPR, the EEA Standard Contractual Clauses (incorporated by reference pursuant to clause 2.4) shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA, and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in the Agreement.

- 2.6 The Client acknowledges and agrees that certain Processors or Controllers engaged by FTI under paragraph 2.3 may be located in places that may require cross-border transfers of Personal Data. In respect of transfers by FTI to such Controllers or Processors, FTI will take steps in accordance with the Data Protection Laws to ensure an adequate level of protection for the Personal Data Processed by such Processors or Controllers. Where such a Controller or Processor notifies FTI that it may no longer be able to provide an adequate level of protection in accordance with Data Protection Laws, FTI shall independently assess the level of protection provided and, where necessary, shall take mitigating steps to improve the level of protection or, where this is not possible, terminate the transfer.
- 2.7 The Client acknowledges that FTI's email records are replicated onto a Microsoft 365 Cloud system in the United States of America and the Client hereby consents that any Personal Data that is provided to FTI by email will be replicated accordingly. To the extent that the Client wishes to transmit certain information or data to FTI and the Client objects to that data being replicated in accordance with this paragraph, the Client will use a communication or transmission method other than e-mail or will use an alternative e-mail system.



SCHEDULE B

FTI CONSULTING CALIFORNIA DATA PROTECTION SCHEDULE

This California Data Protection Schedule ("Schedule") forms part of the contract for services to which it is an attachment (the "Contract") between the client party identified in the Contract (the "Client") and the relevant FTI Consulting group entity identified in the Contract ("FTI"). FTI will be functioning as a service provider.

1. Processing of Personal Information.

In connection with FTI's provision of services to Client under the Contract, if FTI receives any personal information (as such term is defined under the California Consumer Privacy Act) from or on behalf of Customer, then FTI:

- (a) will only process such personal information for the purpose of providing the services;
- (b) will not retain, use, or disclose such personal information for any purpose other than to perform the services or outside of the direct business relationship between FTI and Client;
- (c) will not sell, rent, release, disclose, disseminate, make available, transfer or otherwise communicate such personal information to any third party for monetary or other valuable consideration; and
- (d) certifies that it understands the restrictions on its processing of such personal information as set forth in this sentence, and will comply with them.

FTI may disclose personal information to FTI's service providers in connection with such service providers providing services to FTI, and FTI may permit such service providers to process personal information as necessary for FTI to provide the services to Client.



Annex 1: Description of Personal Data Processing

This Annex includes certain details of the Processing of Personal Data by FTI under the Principal Agreement.

1. Subject matter and duration of the Processing of the Personal Data

The subject matter and duration of the Processing of the Personal Data are set out in the Principal Agreement and this Schedule.

2. The nature and purpose of the Processing of the Personal Data

FTI is engaged to provide Services to Client which involve the Processing of Personal Data. The scope of the Services are set out in the Principal Agreement, and the Client Personal Data will be Processed by FTI for purposes determined by it, in connection with the delivery of those Services and compliance with the terms of the Principal Agreement, including this Addendum, as well as applicable laws.

3. The types of the Personal Data to be Processed

Client customer or employee information which may be collected in the course of delivering consulting and advisory services to Client, including name, title, gender, personal contact details (address, telephone number, email address), work address, work email, work telephone numbers, job title, and other types of Personal Data supplied by the Client to FTI pursuant to the Principal Agreement.

4. The categories of Data Subject to whom the Personal Data relates

The categories of Data Subjects are determined by the nature of the client engagement, the details of which are covered in the Principal Agreement.

5. The obligations and rights of Client

The obligations and rights of Client are set out in the Principal Agreement and this Schedule.

6. Frequency of Restricted Transfers (where applicable):

As necessary to deliver Services for the duration of the Principal Agreement.

7. The period for which Personal Data subject to Restricted Transfers will be retained (where applicable):

In accordance with FTI's data retention policies, copies of which are available upon request.



Annex 2: Technical and Organizational Security Measures

FTI Consulting maintains the following technical and organizational security measures when processing Personal Data for its clients.

- Measures of pseudonymisation and encryption of personal data

When data at rest leaves our direct control (such as backup tapes, removable hard drives, etc.) the data is encrypted using AES 256-bit encryption. All laptops utilize full disk encryption. Data that is in transit over public circuits is encrypted in transit using SSL. FTI Consulting additionally deploys firewalls throughout its networks to allow and deny specific network traffic using key indicators such as source/destination address, source/destination port, etc.

- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

FTI requires new employees/contractors to acknowledge receipt of the following policies including: Code of Ethics and Business Conduct, Anti-Corruption Policy, Acceptable Use of Technology Resources, Confidentiality Agreement, Employee Handbook Policy on Inside Information & Insider Trading, and Time Recording Policy.

FTI Consulting has a documented policy for business continuity and disaster recovery that has been approved by management, communicated properly and is maintained and reviewed. The general details are reflected in the FTI Consulting Information Security Policy. The recovery point objective exceeds 4 hours and the recovery time objective exceeds 24 hours. The specific tools used for backups vary by region.

- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

FTI has access to all major vendor security bulletins and have controls over identifying, scheduling, testing, and deploying patches. The deployment time is 14 days for high and within 24 hours for critical/emergency patches.

FTI has controls over identification of vulnerabilities, risk ranking, reporting, and remediation. This includes perimeter vulnerability scans that must be performed at least quarterly and semi-annual internal vulnerability scans that cover workstations, servers, and network devices.

FTI performs internal penetration test to identify flaws in the internal security controls that could allow an attacker to surreptitiously gain access to sensitive data and/or disrupt critical business systems. The organization must also perform external network penetration test to identify potential vulnerabilities which could be exploited to gain access to systems and data or to establish a foothold into internal network from which to launch further attacks.

FTI's cybersecurity team tracks the resolution of vulnerabilities. Vulnerabilities that are not resolved as part of patching cycles must be tracked on a vulnerability log or similar mechanism.

- Measures for user identification and authorization

FTI uses unique IDs and if generic IDs should be disabled unless there is an approved security exception. FTI users authenticate through Active Directory (AD), SSO used when possible, and remote connection requires two factor authentication and leverages FTI's Corporate DUO two factor technology. Duo Security generates passcodes (similar to a PIN Code) to mobile devices for login and can receive push notifications for easy



updates. Duo Security is integrated with OneLogin (our SSO platform) providing a unified authentication solution.

Privileged and remote access must include multi-factor authentication and secure mechanisms (e.g., TACACs+, RADIUS) must be used on all network devices.

FTI password complexity (i.e. characters, length), lockout settings, expiration settings meets the following requirements:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9,!@#\$%^&*()_+|~-=\{\}[];:"<>?,./)
- Contains at least 12 characters for standards accounts and 15 characters in length for admin accounts
- Must be changed at least every 90 days
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on Confidential Information, names of family, etc.
- User accounts are locked after 10 unsuccessful logins. Account lockout for 30 mins. Reset after 30 mins.
- Password history - 24 passwords remembered

Passwords are stored protected in an encrypted format.

- Measures for the protection of data during transmission and measures for the protection of data during storage

FTI has Data Loss Prevention (DLP) and extrusion prevention tools that restrict sending sensitive data over unsecure mail. Anomalies that exceed the normal traffic patterns are noted and appropriate action is taken to address them.

FTI protects data in transmission which include the following acceptable methods:

- Email: Transport Layer Security ("TLS") Internet protocol, which provides security for all email transmissions over the public Internet may be setup with using opportunistic or mandatory TLS connections. Only TLS 1.2 or TLS 1.3 is acceptable.
- "Mailbox to mailbox" encryption that secures email messages and electronic files (using 256-bit AES encryption).
- Secure FTP: FTP utilizes TLS or SSH to allow us to share data with clients securely over the Internet. Only TLS 1.2 or TLS 1.3 is acceptable.
- External Encrypted Drive: Must use FIPS 140-2/AES 256-bit encryption or stronger.
- File Stores: Matter/Engagement related files stored centrally on the network are secured so that only those explicitly authorized can access the files.

FTI stores data in an environment that is not internet facing and segregated from the demilitarized zone by a firewall. The data must be logically segregated from other client or corporate data. Different tools may be employed depending upon the nature and/or location of the work.

- Measures for ensuring physical security of locations at which personal data are processed

Specific physical security provisions vary depending on office location, however, as per the Information Security policy, access to company premises, including delivery and loading areas, must require badge access.



Badge access is managed by local facilities or ITG, who use a badge kiosk to produce access badges. All badge issuances and updates require management approval.

- Measures for ensuring events logging

FTI logs activity which is stored for 7 years. Data is logged at sufficient level (i.e. user ID, activity) and logging is enabled for the entire environment. The logging must provide relevant information (i.e. authorized & unauthorized attempts, remote access). System event and audit logs should capture the following events as applicable:

- Authentication failures
- Software or service failures
- Logon and use of privileged IDs
- Database changes
- Adding/deleting users
- Password Changes
- Adding/deleting groups and/or users associated with groups
- Changing audit log configuration or disabling audit subsystem

FTI uses SecureWorks which provides a Security Incident and Event Management (SIEM). The foundation of the SIEM includes Red Cloak endpoint event logs analysis, which includes an industry-leading assessment of current and zero-day threats and vulnerabilities.

- Measures for ensuring system configuration, including default configuration Measures for internal IT and IT security governance and management

FTI has processes in place to confirm compliance with configuration standards. This includes a process for newly created device (i.e., checklist), at least annual reviews and hardening, removal of unnecessary / insecure services, and alarms set for key events (i.e. change in security group, configuration).

- Measures for certification/assurance of processes and products

FTI holds the Certified Enterprise designation from Verizon Cybertrust and participates in their Security Management Program (SMP). The SMP is a comprehensive security risk reduction and certification program that addresses all aspects of proactive information security, from network and system analysis to physical and policy inspection. The cornerstone of SMP is the International Standards Organization (ISO) standard 27002.

As part of the Cybertrust Third Party assessment schedule, FTI Consulting's Global Cybersecurity and Privacy function undergoes the following reviews by the Verizon Security Certification organization:

- Policy Review — evaluates the documentation and inspects the contents of key security policies — Annually.
- Process and Procedure Validation — Annually.
- Physical Inspection — evaluates the implementation of security controls in the physical environment surrounding critical network infrastructure, including doors, HVAC, entry logs, power redundancy, etc. — Annually.
- External Risk Assessments (Network and System-level scans) — Quarterly identifies possible risk areas in an organization's external network infrastructure and assesses its consistency with key controls.
- Penetration testing (External and Internal – Network and System-level) is conducted by a separate third-party — Annually.

Individual business units may hold additional certifications or use tools that are supported by additional certifications.



- Measures for ensuring data minimisation

FTI only acquires data for the intended purpose by working with the client or business partner to ensure only the minimum amount of necessary data is obtained.

- Measures for ensuring data quality

FTI Consulting is dedicated to providing its clients with high quality services that meet our standards of excellence and integrity. The quality of the work for each of our clients is monitored by the Senior Managing Directors responsible for each engagement along with the highly qualified colleagues in their practice teams and business segments. On a broader level, FTI sets the tone for our global organization in our Code of Conduct (<https://www.fticonsulting.com/~/media/Files/us-files/our-firm/guidelines/fti-code-of-conduct.pdf>) which discusses our commitment to quality throughout, and in particular in our Statement of Values.

FTI takes into account the principle of purpose limitation, while making sure that the data is adequate, relevant and not excessive for the legitimate purpose. FTI enables data subjects to exercise their rights, including the rights of access and, as appropriate, the rectification, erasure or blocking of Personal data and keep data accurate, and not retain it any longer than necessary.

- Measures for ensuring limited data retention

FTI has a records retention policy that ensures records are retained for required and necessary periods of time; providing that records which are no longer useful are properly destroyed; and providing that records to be retained are stored methodically and economically. FTI uses their reasonable and best efforts to prevent the premature destruction of Records. The organization must have processes to return data upon end of contract and destroy data using appropriate mechanisms upon Department of Defense (DoD) and National Institute of Standards and Technology (NIST) standards for all data bearing devices.

- Measures for ensuring accountability

FTI has a defined process to resolve complaints about privacy and its collection or use of personal information in compliance with the EU-US Privacy Shield Principles. FTI has measures in place to ensure complaints are resolved within 1 month. Unless otherwise dictated by local law, the exact number of days to comply with a request varies, depending on the month in which the request was made and is calculated based on the day the request is received plus one (regardless of whether the day is a working day or not) until the corresponding calendar date in the next month.

- Measures for allowing data portability and ensuring erasure

FTI receives requested Personal Data directly or provide access to a tool which allows the requestor to extract the information themselves using a self-service type model.

The Personal Data requested is required to be provided in a format and structure which is commonly used and machine-readable. The following machine-readable formats:

- CSV: (Comma separated values) a format that stores tabular data (numbers and text) in plain-text form;
- PDF: (Portable Document Format) a file format used mainly to represent documents such that layout will stay the same independent of the system environment;
- XML: (eXtensible Markup Language) a markup language that defines a set of rules for encoding documents in a format that can be both human and machine readable;



- JSON: (JavaScript Object Notation) a machine-readable data format derived from the JavaScript language used for representing simple data structures and associative arrays; or
- HTML: (HyperText Markup Language) the main markup language for displaying web pages and other information in a web browser.

FTI has a data erasure process in place to track and manage responses, and, as necessary, provide updates to the relevant regulatory authority and/or input into management reports. The organization must verify the identity of the data subject before disclosing any personal information. The organization should only refuse to comply with an erasure request if it is "manifestly unfounded or excessive" or, alternatively may elect to charge a "reasonable fee." The response is in written communication together with the documents containing the proper erasure of data.